OMB # 0970-0568
Expiration Date: 04/30/2024

SECURITY v1.0

Introduction

To build and maintain a resilient CCWIS in the face of cyberattacks and other data security threats, title IV-E agencies (agencies) need to implement a holistic information-security and risk-management approach that includes significant security controls to strengthen the technology system and the operating environment. Agencies need to manage and mitigate information security risk at the organizational and information systems level.

This self-assessment tool assists agencies with meeting security standards and goals when designing and developing CCWIS modules and systems.

Tool Format

This self-assessment tool is divided into sections as outlined on the chart below. Every question has a unique *Element #* for easy reference. Please refer to the instructions in Technical Bulletin #7 or contact your federal analyst if you have questions about the tool or a specific element.

Section	Element #
Overview and Background Information	L.A.xx
Self-Assessment – Part 1 – *Identification*	L.B1.xx
Self-Assessment – Part 2 – *Protection*	L.B2.xx
Self-Assessment – Part 3 – *Monitoring and Detection*	L.B3.xx
Self-Assessment – Part 4 – *Response*	L.B4.xx
Self-Assessment – Part 5 – *Recovery*	L.B5.xx
Resources	L.C

A. Overview and Background Information

In the Overview and Background Information section, agencies may collect information on the overall CCWIS (or collection of modules if appropriate) and its security environment. *If a question is not applicable to the system or module you are evaluating, indicate "N/A" and provide a reason it is not applicable.*

L.A.01 Date this assessment was completed.

L.A.02 Name of the CCWIS or module(s) included in this self-assessment.

L.A.03 Describe or attach documentation that details where the system code and data are hosted (such as on-premise, cloud, etc.). Documentation may include system boundary diagrams; inventories of hardware and software components used to transmit, process, or store CCWIS information; and policies and procedures that demonstrate approaches to physical and virtual security. Indicate the date(s) when the agency last updated the documentation.

L.A.04 Describe or attach documentation that details dedicated exchanges and data sharing between this CCWIS and other information systems, both within the agency and external to the agency, including ports, protocols, services utilized, and data shared. Artifacts may include documentation such as a network and data-flow diagram, system interconnection security agreements, and intra/inter-agency data sharing agreements.

L.A.05 Provide any additional comments as background regarding the security of your system or module.

B. Self-Assessment

In this section, the agency may document components, factors, and design elements of the functions(s) or exchanges that support the security goals of the CCWIS. If the agency has additional goals, please include them below and add new rows as needed. We encourage agencies to simplify their responses by referencing previously submitted documentation, such as APDs or attaching security plans, policies, and protocols.

If a goal is not applicable, indicate "N/A" and provide a reason.

Part 1 – Identification

Assess whether the agency has the organizational understanding to manage cybersecurity risk to the CCWIS and related assets and data.

#	Security Goal	Evidence the CCWIS Supports the Goal
L.B1.01	*Effective asset management*. System data, personnel, devices, components, external information systems, and facilities are identified and managed consistent with their relative importance to agency business objectives and risk strategy.	*Typically demonstrated in association with development of a system component inventory, interconnection security agreements, and documentation of roles and responsibilities.*
L.B1.02	*Security informed by governance and business environment.* Agency governance, mission, objectives, stakeholders, and activities are identified and used to inform security roles, responsibilities, and risk management decisions pertaining to the system.	*Typically demonstrated by the establishment of comprehensive security policy and procedures or adoption of an industry standard security framework, such as the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).*
L.B1.03	*Active risk management*. The agency understands the security risks to operations, assets, individuals, and supply chains.	*Typically demonstrated in association with a risk assessment that addresses the method and frequency of assessments along with responsible parties and timeframes for addressing risks and issues.*

Part 2 – Protection

Assess whether the agency has developed and implemented the appropriate safeguards to protect the integrity of the CCWIS and the data contained within from external and internal threats.

#	Security Goal	Evidence the CCWIS Supports the Goal
L.B2.01	*Effective access control*. The agency limits system access to authorized users, processes, or devices.	*Typically demonstrated, in association with a system security plan (SSP), through implementing associated security controls. The response should address how the agency adds, maintains, and terminates user accounts.*
L.B2.02	*Security awareness and training*. The agency provides personnel and partners with security-awareness and security role-based training.	*Typically demonstrated with training plans, training schedules, and curricula content.*
L.B2.03	*Effective data security*. The agency manages information and records through physical and electronic measures to protect the confidentiality, integrity, and availability of information.	*Typically demonstrated in association with a developed Privacy Impact Assessment (PIA), examples of which are found at https://www.hhs.gov/pia/index.html, and in association with activities to, for example, conduct privacy awareness training, minimize the collection and retention of PII, and display Privacy Act Statements.*
L.B2.04	*Established information protection processes and procedures*. The agency maintains security policies, processes, and procedures to manage protection of the system and associated assets.	*Typically demonstrated through the establishment of baseline configurations and configuration change control, adherence to an implemented system development lifecycle (SDLC), comprehensive backups, and the establishment, testing, and continuous improvement of protection, response, and recovery policy.*
L.B2.05	*Regular maintenance*. The agency performs maintenance and repairs of the system and associated components consistent with title IV-E agency policies and procedures.	*Typically demonstrated with reference documentation and schedules of recent updates and repairs. Documentation should include the current version of any software, hardware, and cloud-based services used for the CCWIS.*
L.B2.06	*Consistent application*. All data within the CCWIS has the same security impact level.	*Typically demonstrated, in association with the SSP, through the associated controls that govern the security impact level for CCWIS data.*

Part 3 – Monitoring and Detection

Assess whether the agency has developed and implemented the appropriate safeguards to identify the occurrence of a cybersecurity event associated with the CCWIS.

#	Security Goal	Evidence the CCWIS Supports the Goal
L.B3.01	*Detection of anomalous activity*. The agency implements, maintains, and tests detection mechanisms, processes, and procedures to ensure awareness and understanding of anomalous activity and events.	*Typically demonstrated through the collection, correlation, and analysis of event data from multiple sources and sensors.*
L.B3.02	*Security continuous monitoring*. The agency assesses security controls and information security-related risks at a frequency sufficient to verify the effectiveness of protective measures and support the agency's risk-based decisions.	*Typically demonstrated through frequently updated reports or real-time dashboards that provide security-related information that is specific, measurable, actionable, relevant, and timely.*

Part 4 – Response

Assess whether the agency has developed and implemented the appropriate procedures to take when a cybersecurity event associated with the CCWIS has been detected.

#	Security Goal	Evidence the CCWIS Supports the Goal
L.B4.01	*Coordinated response planning*. Response activities are planned and executed in coordination with internal and external stakeholders consistent with laws and policies, and informed through alerts, advisories, and information sharing to achieve broad cybersecurity situational awareness.	*Typically demonstrated in association with developed Incident Response (IR) and Contingency Plans.*
L.B4.02	*Comprehensive response analysis*. The agency analyzes response and recovery activities to ensure security incidents, including	*Typically demonstrated through incident response and breach protocols in association with after-the-fact investigations and reporting of security*

#	Security Goal	Evidence the CCWIS Supports the Goal
	breaches, are understood and mitigated. The agency incorporates lessons learned to improve response plans.	*incidents.*

Part 5 – Recovery

Assess whether the agency has developed and implemented the appropriate activities to maintain plans for continuity of operations and to restore any system capabilities or services impaired due to a cybersecurity event or other interruption.

#	Security Goal	Evidence the CCWIS Supports the Goal
L.B5.01	*Coordinated recovery planning*. The agency plans and executes response activities to ensure restoration of systems affected by security incidents in coordination with internal and external stakeholders. The agency incorporates lessons learned to improve response plans.	*Typically addressed in association with the development of a Continuity of Operations or Contingency Plan.*

C. Resources

The Resources section describes security techniques and best practices agencies may wish to consider when creating and maintaining a secure CCWIS environment. *Links provided are current at the time of publication. If a link is no longer valid, please communicate this to ACF.*

Resource 1 – Risk Management

Resource 2 – Cybersecurity

Resource 3 – Encryption

Resource 4 – Password Management

Resource 5 – Multi-Factor Authentication (MFA)

Resource 6 – Defending Against Ransomware

Resource 7 – Phishing Awareness

Resource 8 – Data Breaches: Detection and Response

C. Resources

Resource 1 – Risk Management

Agencies may use the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) to manage security and privacy risks. The RMF provides a dynamic and flexible approach to managing risk in diverse environments with complex and sophisticated threats, evolving missions and business functions, and changing system and organizational vulnerabilities.

- **NIST SP 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**
  https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
  This publication describes the RMF and provides guidelines for managing security and privacy risks and applying the RMF to information systems and organizations.

Resource 2 – Cybersecurity

State, Local, Tribal, and Territorial (SLTT) Resources

DHS offers a broad set of cybersecurity resources to SLTT governments.

- **DHS Cybersecurity Services Catalog for SLTT Governments**
  https://www.us-cert.gov/sites/default/files/c3vp/sltt/SLTT_Hands_On_Support.pdf
  This catalog lists and describes cybersecurity services available to the SLTT community. All services featured in the catalog are voluntary, non-binding, no cost, and available to stakeholders upon request.

- **Assessments: Cyber Resilience Review (CRR)**
  https://www.us-cert.gov/resources/assessments
  The Cyber Resilience Review (CRR) is provided on a voluntary, no-cost basis for SLTT governments. The CRR offers insights into an organization's operational resilience and cybersecurity capabilities and can be conducted as a self-assessment or as an on-site session facilitated by DHS cybersecurity professionals.

Federal Risk and Authorization Management Program (FedRAMP)

The FedRAMP program provides U.S. government agencies with a standardized approach to security for cloud products and services. Agencies can benefit from this federal program by choosing a FedRAMP-compliant cloud-solution provider (CSP), which can save time and effort while improving security.

- **FedRAMP Marketplace**
  https://marketplace.fedramp.gov/
  The FedRAMP Marketplace website lists all products and all vendors that hold a FedRAMP designation.

C. Resources

Resource 3 – Encryption

Encrypting information for transmission or storage protects the information from unauthorized disclosure and modification. Agencies should encrypt sensitive information both in transit and at rest. Cryptographic mechanisms implemented to protect information integrity include cryptographic hash functions, checksums, and message authentication codes.

- **NIST Special Publication 800-175B, Rev 1: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf
  This NIST publication details federal encryption standards and guidelines, cryptographic algorithms and services, and key management standards. Agencies can implement recommendations to ensure that their encryption mechanisms follow best practices.

- **NIST Special Publication 800-52, Rev 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
  Transport Layer Security (TLS) provides mechanisms to protect data during electronic dissemination across the internet. This document guides the selection and configuration of TLS protocol implementations while effectively using Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms.

Resource 4 – Password Management

Traditional password management guidelines have been shown to cause problems and NIST guidelines include recommendations that differ from previous advice. For example, instead of enforcing strict password composition requirements, NIST now recommends screening passwords against lists of commonly used or compromised passwords because users employ predictable methods for satisfying composition rules, which limits their benefit. NIST also recommends against forcing users to change passwords periodically because users often choose a new password by applying a set of common transformations to their old password, and this provides a false sense of security.

- **NIST SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management**
  https://pages.nist.gov/800-63-3/sp800-63b.html
  This publication includes a comprehensive list of best practices for password management, and the supplemental FAQ addresses many common questions.

- **List of passwords previously exposed in data breaches**
  https://haveibeenpwned.com/Passwords
  This website maintains a list of more than 600 million real-world passwords previously exposed in data breaches. The list is freely available for download and can also be searched using the provided k-anonymity API.

C. Resources

Resource 5 – Multifactor Authentication (MFA)

Using multifactor authentication enhances security by making it more difficult for attackers to gain access even if they correctly guess an account password. MFA provides a strong defense against many types of attacks, including phishing, malware, and brute force attacks.

MFA requires the use of more than one distinct authentication factor to achieve authentication, and the factors fall into three categories: something you know (such as a password or PIN), something you have (such as a smart card or hardware token), or something you are (such as a fingerprint).

- **Selecting and Safely Using Multifactor Authentication Services**
  https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/CSI_MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF

  This whitepaper identifies criteria for government agencies to consider when researching MFA services.

- **NIST SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management**
  https://pages.nist.gov/800-63-3/sp800-63b.html
  This publication provides a comprehensive list of authenticators, including detailed descriptions and information about their strengths and usability considerations.

Resource 6 – Defending Against Ransomware

Ransomware and other destructive malware can alter or destroy critical data, rendering it unusable and causing the complete shutdown of business operations. Ransomware incidents increased sharply in 2019, disrupting hundreds of government agencies, educational institutions, and healthcare providers. Defending against these increasingly sophisticated attacks requires preparation before an incident occurs to help mitigate their impact.

- **NIST SP 1800-25: Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events**
  https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect
  These draft guidelines include a "how to" guide to implement best practices to identify assets and vulnerabilities and have defenses in place to reduce the impact of destructive attacks.

- **NIST SP 1800-26: Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events**
  https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond
  These draft guidelines include a "how to" guide to implement best practices to quickly detect and mitigate data corruption incidents and reduce their potential impact.

C. Resources

Resource 7 – Phishing Awareness

Phishing refers to a type of social engineering attack that uses deceptive emails to trick people into revealing sensitive information, such as account credentials, leading to malware installation and data loss. Raising user awareness is vital in defending against phishing attacks, and simulated phishing emails based on real-world threats provide a key method to train users to know what to look for and how to report it.

- **No Phishing beyond This Point**
  https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6605070/
  This paper describes guidelines for implementing simulated phishing based on four years of data gathered by a NIST research team in a real-world work environment, which revealed that the more the context of the email seems relevant to a person's life or job responsibilities, the harder it is for them to recognize it as a phishing attack.

Resource 8 – Data Breaches: Detection and Response

States, tribes, and local agencies are responsible for the security of information within child welfare information systems and should proactively mitigate risks associated with the inadvertent loss or unapproved disclosure of confidential information. As title IV-E child welfare information systems mature and government agencies continue to face significant security threats, the need to review and implement comprehensive data security programs is paramount. Agencies are encouraged to formalize data breach response plans to continually monitor and assess protocols, confidentiality requirements, system vulnerabilities, and risk mitigation strategies.

- **ACYF-CB-IM-15-04: State and Tribal Child Welfare Information Systems, Information Security Data Breach Response Plans**
  https://www.acf.hhs.gov/cb/resource/im1504
  Key management practices title IV-E agencies may consider when developing plans to detect or respond to data breaches.